(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000047988 A**

(43) Date of publication of application: **18.02.00**

(51) Int. Cl **G06F 15/00**

(21) Application number: **10212225**

(22) Date of filing: **28.07.98**

(71) Applicant: **HITACHI LTD**

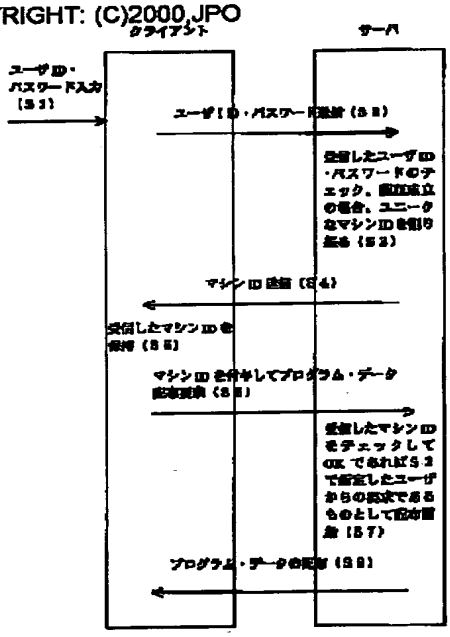
(72) Inventor: **TOZONO RYOJI**

(54) **CERTIFYING METHOD BY MACHINE ID**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a certifying method capable of performing an operatorless job operation even the distribution to an unmanned terminal in the night requiring a certificate by unnecessitating log-in operation based on a user identifier (ID) password for every job execution request.

SOLUTION: Concerning this certifying method, when a client machine is logged in by the user ID password certified on the side of a server or when the normality is proofed by receiving a client certificate after a certificate is transmitted to the server, a machine ID to be uniquely determined is distributed from the server for each client machine. By using the distributed machine ID for the following client certification, the log-in based on the user ID password for each job execution request from the client is unnecessitated and the certifying function of the client machine itself can be provided.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－47988
（P2000－47988A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ　５Ｂ０８５

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平10－212225

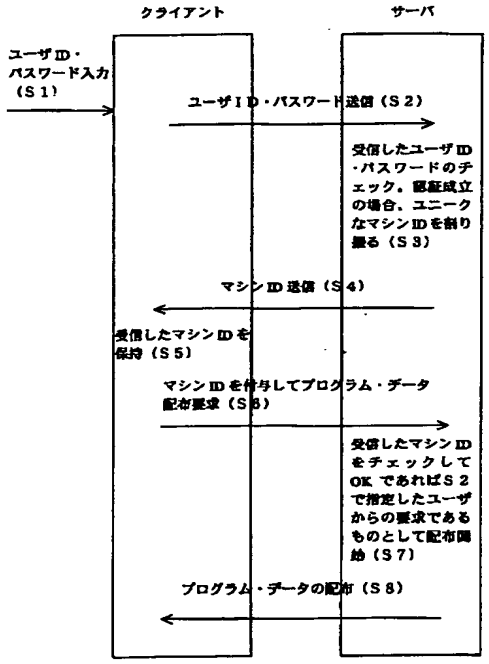
(22)出願日　平成10年７月28日(1998.7.28)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　東園　良二
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(74)代理人　100096954
弁理士　矢島　保夫

Ｆターム(参考)　5B085 AC03 AE01 AE04 AE23

(54)【発明の名称】　マシンＩＤによる認証方法

(57)【要約】
【課題】インターネット／イントラネット環境でクライアントからサーバに対して配布要求等を行う場合、サーバに対してその都度配布認証を受けるため、クライアントユーザは，必ずユーザＩＤ・パスワードでログインする必要があった。またプログラムやデータ配布業務の場合は、クライアントのユーザ（人）ではなくマシンに配布するというニーズがあるが、クライアントマシンにログインするユーザ（人）ではなくクライアントマシン自体を認証する機能がなかった。
【解決手段】前記課題を解決するために，本発明では、サーバ側で認証されているユーザＩＤ・パスワードでクライアントマシンにログインするかまたは証書をサーバに送信後にクライアント認証を受け、正当性が証明された場合に、サーバからクライアントマシン単位に一意に決まるマシンＩＤを割り振る。その後のクライアント認証には、割り振られたマシンＩＤを使用する事により、クライアントからの業務実行要求毎のユーザＩＤ・パスワードによるログインを不要にするとともに、クライアントマシン自体の認証機能を提供する。



【特許請求の範囲】

【請求項１】認証を行う計算機と複数の認証される計算機とがネットワークで接続されたシステムにおける認証方法であって、

前記認証される計算機において入力されたユーザＩＤとパスワードを前記認証する計算機へ送信するステップと、

前記認証する計算機において、受信した前記ユーザＩＤとパスワードが正当なユーザのものであることを認証するステップと、

正当なユーザと認証されたときには、前記認証する計算機から前記認証される計算機へ、前記認証される計算機を特定する識別子であるマシンＩＤを送信するステップと、

前記マシンＩＤが送信された以降は、前記認証される計算機から前記認証を行う計算機に前記マシンＩＤを送信することにより前記認証される計算機を認証するステップとを備えたことを特徴とするマシンＩＤによる認証方法。

【請求項２】認証を行う計算機と複数の認証される計算機とがネットワークで接続されたシステムにおける認証方法であって、

前記認証される計算機において入力されたユーザＩＤと証書を前記認証する計算機へ送信するステップと、

前記認証する計算機において、受信した証書により前記ユーザＩＤのユーザを認証するステップと、

正当なユーザと認証されたときには、前記認証する計算機から前記認証される計算機へ、前記認証される計算機を特定する識別子であるマシンＩＤを送信するステップと、

前記マシンＩＤが送信された以降は、前記認証される計算機から前記認証を行う計算機に前記マシンＩＤを送信することにより前記認証される計算機を認証するステップとを備えたことを特徴とするマシンＩＤによる認証方法。

【請求項３】請求項１または請求項２において、前記認証される計算機から前記マシンＩＤを受信した前記認証する計算機は、前記マシンＩＤの認証を行うとともに、当該マシンＩＤを割り振ったときの認証要求元ユーザを認識し、要求された業務が当該ユーザの実行許可業務であるか否かをチェックすることを特徴とするマシンＩＤによる認証方法。

【請求項４】請求項１または請求項２において、前記マシンＩＤのバックアップを取得するステップと、該バックアップからマシンＩＤを回復するステップとを備えたことを特徴とするマシンＩＤによる認証方法。

【請求項５】請求項１または請求項２において、前記認証する計算機に登録されている前記マシンＩＤを、前記認証する計算機または前記認証される計算機側からの操作により削除するステップを備えたことを特徴とするマシンＩＤによる認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク上に分散配置された複数の認証される側のマシンから認証を行う側のマシンにアクセスして業務を実行する環境で、認証される側のマシン単位に割り振られた一意なマシンＩＤ（識別子）により認証する認証方法に関する。

【０００２】

【従来の技術】近年、インターネット／イントラネット環境の普及に伴い同環境で業務を実行する場合、例えばプログラムやデータの配布等に関しては、従来サーバ側から複数のクライアント側に対してブロードキャスト的に配布していた形態から、クライアントユーザまたはクライアントシステムがサーバ側に能動的に問合わせを発行しサーバ側はその問合わせに対して応答する問合わせ応答型の配布を行う形態が増えてきている。

【０００３】この様な形態では、クライアント（認証される側)は、ネットワークを介してサーバ（認証する側）に配布要求を行う際に、自分自身の正当性を証明する（クライアント認証を受ける）必要がある。ネットワークにおけるクライアントの認証方法に関しては、例えば特開平２－１６６６９号公報の「セキュリティ方式」のように、クライアント側のユーザが入力したユーザＩＤおよびパスワードをサーバ側に送信し、サーバ側でその内容をチェックする事で、クライアントの正当性を証明する方法がある。このマシン認証をもって、当該マシンへのプログラムやデータの配布が実現される。また、特開平５－３５６７８号公報の「ユーザ認証方式」のように、パスワードの機密性を高めるためにパスワードをネットワーク上に流さずにログイン可能とする方式がある。

【０００４】

【発明が解決しようとする課題】このようにインターネット／イントラネット環境でクライアントからサーバ側に対して業務の実行要求、例えばプログラムやデータの配布要求を行う場合、サーバ側に対してその都度配布認証を受ける必要があるため、クライアント側のユーザは、必ず配布要求時毎に、サーバ側のデータベースに登録してあるユーザＩＤ（またはユーザＩＤおよびパスワード）でログインする必要がある。このとき、例えば大容量のプログラムをクライアントに配布したい場合、回線トラフィックが少ない夜間に配布を実施しようとするためには、オペレータが夜中にログインして配布要求するか、クライアントマシンを夜中の間認証されたユーザＩＤ・パスワードでログイン状態（認証を済ませる）にしておき任意のタイミングでクライアントからサーバに自動的に配布要求を行う必要がある。しかし、前者は運用上、後者はセキュリティ上問題がある。

【０００５】またプログラムやデータ配布の場合は、ク

ライアントのユーザ(人)ではなく計算機に配布（その計算機にログイン可能なユーザは共有して使用／参照が可能）する形にしたい、というニーズがあり、このときは認証される計算機にログインするユーザ（人）ではなく計算機自体をサーバ側で認証する機能が必要である。しかし、前述の２つの方法では、クライアントマシン自体の認証方法については記述されていない。

【０００６】本発明の目的は、インターネット／イントラネットといったクライアント認証が必須である環境において、オペレータが夜中にログインしてサーバに業務の実行を要求したり、クライアントマシンを夜中の間認証されたユーザＩＤ・パスワードでログイン状態にしておき任意のタイミングで業務の実行を要求するといった運用上あるいはセキュリティ上の問題がある方法を用いることなく、業務実行要求毎のユーザＩＤ・パスワードによるログイン操作を不要にして、認証を必要とする夜間の無人端末への配布等でもオペレータレスの業務運用を可能にする認証方法を提供する事にある。

【０００７】本発明の他の目的は、クライアントのユーザ(人)ではなく、クライアントの計算機自体をサーバ側で認証する事ができる認証方法を提供する事にある。

【０００８】

【課題を解決するための手段】上記目的を達成するため、請求項１に係る発明は、認証を行う計算機と複数の認証される計算機とがネットワークで接続されたシステムにおける認証方法であって、前記認証される計算機において入力されたユーザＩＤとパスワードを前記認証する計算機へ送信するステップと、前記認証する計算機において、受信した前記ユーザＩＤとパスワードが正当なユーザのものであることを認証するステップと、正当なユーザと認証されたときには、前記認証する計算機から前記認証される計算機へ、前記認証される計算機を特定する識別子であるマシンＩＤを送信するステップと、前記マシンＩＤが送信された以降は、前記認証される計算機から前記認証を行う計算機に前記マシンＩＤを送信することにより前記認証される計算機を認証するステップとを備えたことを特徴とする。

【０００９】請求項２に係る発明は、認証を行う計算機と複数の認証される計算機とがネットワークで接続されたシステムにおける認証方法であって、前記認証される計算機において入力されたユーザＩＤと証書を前記認証する計算機へ送信するステップと、前記認証する計算機において、受信した証書により前記ユーザＩＤのユーザを認証するステップと、正当なユーザと認証されたときには、前記認証する計算機から前記認証される計算機へ、前記認証される計算機を特定する識別子であるマシンＩＤを送信するステップと、前記マシンＩＤが送信された以降は、前記認証される計算機から前記認証を行う計算機に前記マシンＩＤを送信することにより前記認証される計算機を認証するステップとを備えたことを特徴とする。

【００１０】請求項３に係る発明は、請求項１または請求項２において、前記認証される計算機から前記マシンＩＤを受信した前記認証する計算機は、前記マシンＩＤの認証を行うとともに、当該マシンＩＤを割り振ったときの認証要求元ユーザを認識し、要求された業務が当該ユーザの実行許可業務であるか否かをチェックすることを特徴とする。

【００１１】請求項４に係る発明は、請求項１または請求項２において、前記マシンＩＤのバックアップを取得するステップと、該バックアップからマシンＩＤを回復するステップとを備えたことを特徴とする。

【００１２】請求項５に係る発明は、請求項１または請求項２において、前記認証する計算機に登録されている前記マシンＩＤを、前記認証する計算機または前記認証される計算機側からの操作により削除するステップを備えたことを特徴とする。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。

【００１４】図１は、本発明に係るマシンＩＤによる認証方法を適用するためのクライアント／サーバシステムの構成図である。図１において、１は各部門サーバまたはクライアントの上位に位置し、配下の部門サーバやクライアントの認証を行うサーバである。２は上位のサーバに認証を受けたり、また配下の部門サーバやクライアントの認証を行う部門サーバ、３は上位のサーバや部門サーバに認証を受けるクライアントである。本発明は、クライアント３がその上位のサーバ１に認証を受ける場合、クライアント３がその上位の部門サーバ２に認証を受ける場合、部門サーバ２がその上位のサーバ１に認証を受ける場合、および部門サーバ２がその上位の部門サーバ２に認証を受ける場合など、認証が必要な種々の場合に適用可能である。以下図２以降では、クライアントが上位のサーバに認証を受ける場合を例に説明するが、他の場合も同様の構成および処理手順を適用すればよい。

【００１５】図２は、本発明の一実施の形態として、プログラムやデータの配布要求を行う１台または複数台のクライアント２１と、該クライアントからの配布要求受信時に、配布に先立って該クライアントの認証を行うサーバ１２とが、ネットワーク１１を介して接続されている場合の構成例を示す図である。

【００１６】図２において、１１は後述するサーバやクライアント間を物理的・論理的に接続し各種プログラム・データ配布の媒体となるネットワーク、１２はクライアントの認証処理やクライアントへのプログラムやデータの送信処理を行うサーバである。１３はクライアントから送られてきたユーザＩＤ・パスワードやマシンＩＤを認証するクライアント認証処理部、１４はクライアン

トから送られてきたユーザＩＤ・パスワードが認証されたときに、マシンＩＤを割り振るマシンＩＤ制御部、１５はクライアントからの配布要求に応じてプログラムやデータを送信するプログラム・データ送信処理部、１６は外部装置としてクライアント認証やプログラム・データ配布の情報を格納するデータベース、１７はデータベース１６が格納する情報をサーバの主記憶・メモリ上に格納するサーバ情報管理テーブル、１８は外部装置であるデータベース１６またはサーバ内の主記憶・メモリ上に格納されるサーバ情報管理テーブル１７へのアクセスを行う管理テーブルアクセス部、１９はサーバ管理者等がクライアント認証テーブルやマシンＩＤ管理テーブルといった情報を更新・参照するための操作端末である。

【００１７】また、２１はサーバ１２に対してクライアント自身の認証要求やプログラム・データの配布要求を行うクライアントである。２２はクライアントユーザより入力されたユーザＩＤ・パスワードや、認証後にサーバ１２により割り振られたマシンＩＤにより、サーバに認証を要求するクライアント認証要求部である。２３は一度サーバ１２より割り振られたマシンＩＤの削除をサーバ側に要求するマシンＩＤ削除要求部、２４はクライアントユーザやクライアントマシンに関する情報（ユーザＩＤ・パスワード、マシンＩＤ）を管理するクライアント情報管理テーブル、２５はサーバ１２より割り振られたマシンＩＤをＦＤ（フロッピーディスク）等の外部装置２７にバックアップしたり、反対に外部装置２７のバックアップからマシンＩＤを回復するバックアップ取得部／回復部、２６はサーバ１２に対してプログラムやデータの配布を要求しサーバ１２から実際に配布されてきたものを受信処理するプログラム・データ受信処理部、２７はマシンＩＤのバックアップを格納する外部装置、２８はクライアントユーザがサーバ１２より割り振られたマシンＩＤの外部装置２７へのバックアップや、外部装置２７からの回復や、マシンＩＤの削除などの実行を指示するための操作端末である。

【００１８】図３は、図２の構成に適用する本発明に係るマシンＩＤによる認証方法において、クライアント２１から送られてきたユーザＩＤ・パスワードを認証するためのクライアント認証テーブルの例である。クライアント認証テーブルは、認証を許可されたユーザＩＤ（３１）、パスワード（３２）、および実行を許可する業務一覧（３３）を含む。クライアント認証テーブルは、図２のデータベース１６に保持され、サーバ情報管理テーブル１７の１つとして主メモリ上にロードされてアクセスされるテーブルである。

【００１９】図４は、図２の構成に適用する本発明に係るマシンＩＤによる認証方法において、クライアントから送られてきたマシンＩＤを認証するためのマシンＩＤ管理テーブルの例である。マシンＩＤ管理テーブルは、各クライアントマシンに割り振ったマシンＩＤ（４１）、マシンＩＤを割り振ったときの要求元ユーザＩＤ（４２）、およびパスワード（４３）を含む。マシンＩＤ管理テーブルは、図２のデータベース１６に保持され、サーバ情報管理テーブル１７の１つとして主メモリ上にロードされてアクセスされるテーブルである。

【００２０】図５は、図２のようにネットワーク１１を介して接続されているクライアント２１が本発明に係るマシンＩＤによる認証方法によりサーバ１２から認証を受け、要求するプログラム・データの配布を受けるための手順を示している。同図に示すように、まずクライアントユーザまたはクライアントマシンのセットアップ管理者は、クライアント２１においてユーザＩＤ・パスワードを入力する（Ｓ１）。クライアント２１は、入力されたユーザＩＤ・パスワードを１回目の配布要求時に暗号化してサーバ１２に送信する（Ｓ２）。１回目とは、例えばクライアントにおいて、１番始めにプログラムやデータの配布を受けそれらをセットアップするときである。すなわち、最初にプログラムやデータをセットアップするときにユーザＩＤ・パスワードで認証を行い、それ以後は後述するようにマシンＩＤで認証を行う。なお、暗号化の方式は、国際標準の方式でも独自のデータスクランブル方式でも良い。

【００２１】ユーザＩＤ・パスワードを受信したサーバ１２は、復号化の後、そのユーザＩＤ・パスワードがデータベース１６または内部メモリ上のサーバ情報管理テーブル１７中のクライアント認証テーブル（図３）に登録されていて、かつ実行許可業務に「配布」が含まれているか否かをチェックする（Ｓ３）。チェックの結果、そのユーザＩＤ・パスワードが登録済みのものと一致し、かつ配布許可を受けている場合は、正当なクライアントである事を認証し、ユニークなマシンＩＤを割り振り、データベース１６または内部メモリ上のサーバ情報管理テーブル１７中のマシンＩＤ管理テーブル（図４）にそのマシンＩＤおよび認証したユーザＩＤ・パスワードを登録する（Ｓ３）。この場合、受信したユーザＩＤ・パスワードで既にマシンＩＤを割り振り済みであっても、また新たに一意なマシンＩＤを割り振る事ができる。なお、暗号化の方式は、国際標準の方式でも独自のデータスクランブル方式でも良い。

【００２２】次に、サーバ１２は、割り振ったマシンＩＤを暗号化してクライアント２１に送信する（Ｓ４）。なお、ユーザＩＤ・パスワードが登録済みのものと一致しなかった場合は、認証に失敗した事をクライアント２１に通知する。

【００２３】クライアント認証が成功し、ユニークなマシンＩＤを受信したクライアント２１は、復号化の後、その内容をクライアント情報管理テーブル２４中に保持する（Ｓ５）。

【００２４】その後、クライアント２１は、サーバ１２に対して、マシンＩＤを付与してプログラムやデータの

配布要求を送信する（Ｓ６）。なお、マシンＩＤが割り振られた後は、当該クライアントからプログラムやデータの配布をサーバに要求するときには、マシンＩＤを付与して配布要求を送信すればよい。例えば、プログラム的に自動的に配布を行いたい場合は、夜中等のトラフィックが少ないときに自動的に、クライアント情報管理テーブル２４中に保持してあるマシンＩＤを取り出しそのマシンＩＤを付与して配布要求を送信するというようなスケジュールを組むようにすればよい。マシンＩＤを付与して配布要求を行うことは、例えばログインしない状態で自動的に行える。

【００２５】マシンＩＤが付与された配布要求を受信したサーバ１２は、そのマシンＩＤがデータベース１６または内部メモリ上のサーバ情報管理テーブル１７中のマシンＩＤ管理テーブル（図４）に登録されているか否かをチェックする（Ｓ７）。チェックの結果、そのマシンＩＤが登録済みのものと一致した場合は、正当なクライアントである事を認証する（Ｓ７）。このとき、マシンＩＤ管理テーブル（図４）を参照して当該マシンＩＤに対応する要求元のユーザＩＤを求め、クライアント認証テーブル（図３）からそのユーザＩＤのユーザに許可されている実行許可業務を求め、クライアントから要求されている業務が許可されているものであるかをチェックする。要求された業務、ここではプログラムやデータの配布が、許可されていれば、要求のあったプログラムやデータを当該クライアント２１に配布する（Ｓ８）。

【００２６】図６は、図２のようにネットワーク１１を介して接続されているクライアント２１が本発明に係るマシンＩＤによる認証方法によりサーバ１２から認証を受けた後の、受信したマシンＩＤのバックアップの取得およびバックアップからの回復時の手順を示している。同図に示すように、Ｓ１１～Ｓ１４の手順は、図５のＳ１～Ｓ４と同じであるので説明は省略する。

【００２７】クライアント認証が成功し、ユニークなマシンＩＤを受信したクライアント２１は、復号化の後、その内容をＦＤ等の外部装置にバックアップする（Ｓ１５）。マシンＩＤをバックアップしたＦＤ等は、当該クライアントユーザにより保管される。

【００２８】クライアントマシンのクラッシュ等、割り振られたマシンＩＤが破壊された場合や、クライアントユーザが使用するマシンを変更する場合は、マシンＩＤをバックアップしたＦＤ等の外部装置からサーバ認証済みのマシンＩＤを回復する（Ｓ１６）。その後、サーバ１２に対して配布要求を送信するときには、回復したマシンＩＤを付与して配布要求を送信する（Ｓ１７）。Ｓ１７～Ｓ１９の処理は、図５のＳ６～Ｓ８と同じである。

【００２９】図７は、図２のようにネットワーク１１を介して接続されているクライアント２１が本発明に係るマシンＩＤによる認証方法によりサーバ１２から認証を受けた後、クライアントマシンの廃棄等により、マシンＩＤの削除をクライアント２１からサーバ１２に要求する手順およびサーバ１２上からマシンＩＤを削除する手順を示している。同図に示すように、Ｓ２１～Ｓ２４の手順は、図５のＳ１～Ｓ４と同じであるので説明は省略する。

【００３０】クライアント認証が成功し、ユニークなマシンＩＤを受信したクライアント２１において、その後、当該クライアントマシンの廃棄等の必要が生じた場合は、クライアントユーザまたはクライアントマシンのセットアップ管理者は操作端末から自身に割り振られたマシンＩＤの削除をサーバ側に要求する（Ｓ２５）。その指示を受けて、クライアント２１は、マシンＩＤの削除要求をサーバ１２側に送信する（Ｓ２６）。

【００３１】マシンＩＤの削除要求を受信したサーバ１２は、そのマシンＩＤがデータベース１６または内部メモリ上のサーバ情報管理テーブル１７中のマシンＩＤ管理テーブル（図４）に登録されているか否かをチェックし、登録されていたら該当するマシンＩＤを削除する（Ｓ２７）。マシンＩＤを削除したサーバ１２は、クライアント２１側にマシンＩＤの削除を通知する（Ｓ２８）。

【００３２】一方、クライアントマシンのクラッシュなどで当該クライアントマシン側からマシンＩＤの削除要求ができない場合は、サーバ側のシステム管理者は、直接、サーバ１２の操作端末から当該マシンＩＤの削除を要求する（Ｓ２９）。マシンＩＤの削除要求を受けたサーバ１２は、削除要求されたマシンＩＤがデータベース１６または内部メモリ上のサーバ情報管理テーブル１７中のマシンＩＤ管理テーブル（図４）に登録されているか否かをチェックし、存在すれば該当するマシンＩＤを削除する（Ｓ３０）。マシンＩＤを削除したサーバ１２は、サーバ側のシステム管理者の操作端末上にマシンＩＤの削除を通知する（Ｓ３１）。

【００３３】上記実施の形態によれば、マシンＩＤを受信したサーバが当該マシンＩＤを割り振ったときの要求元ユーザを認識し、要求された業務がそのユーザに許可されている業務かどうかをチェックしているので、当該ユーザからの業務実行要求であるものとしてサーバが業務を実行するようにできる。

【００３４】さらに、一度認証する計算機よりマシンＩＤを割り振られたクライアントがクラッシュした場合等でも、あらかじめＦＤ等の外部装置に取得していたバックアップからマシンＩＤを回復する事により、クライアントからのユーザＩＤ・パスワードまたは証書によるマシンＩＤの再取得を不要にすることができる。

【００３５】また、一度サーバよりマシンＩＤを割り振られたクライアントがクラッシュまたは廃棄された場合等に、サーバ側に不要となったマシンＩＤを残存させないように、サーバ側またはクライアント側からの操作に

よりマシンＩＤの削除が実行できる。

【００３６】なお、上記実施の形態では、ユーザＩＤとパスワードにより最初の認証を行う例を説明したが、ユーザＩＤとパスワードによる認証の代わり、あるいはそれに加えて、証書による認証方法を用いても良い。証書とは、例えば、その証書の所有者の公開鍵をユーザＩＤ等の幾つかの情報とともに、認証局の秘密鍵を用いて暗号化したデータ（いわゆるディジタル署名により偽造不可能な形にしたデータ）である。他者は、認証局の証明書（公開鍵）によって該証書のディジタル署名を確認することで、その証書の正当性を確認できる。

【００３７】

【発明の効果】本発明によれば、ネットワークを介して分散しているクライアントマシンからのサーバマシンへの業務実行要求に対する認証方法において、サーバへの初回要求時にユーザＩＤ・パスワードにより認証を受けたクライアントマシンが、２回目以降は初回認証時に割り振られたマシンＩＤを使用して業務の実行要求に対する認証を受けるようにしているので、業務実行要求毎のユーザＩＤ・パスワードによるログイン操作を不要にすることができる。したがって、オペレータが夜中にログインしてサーバに業務の実行を要求したり、クライアントマシンを夜中の間認証されたユーザＩＤ・パスワードでログイン状態にしておき任意のタイミングで業務の実行を要求するといった運用上あるいはセキュリティ上の問題がある方法を用いることなく、認証を必要とする夜間の無人端末への配布等でもオペレータレスの業務運用を可能にする。また、クライアントのユーザ(人)ではなく、クライアントの計算機自体をサーバ側で認証することができる。

【図面の簡単な説明】

【図１】本発明のマシンＩＤによる認証を行うためのクライアント／サーバシステムの構成図である。

【図２】本発明の実施の形態として一台のクライアントと一台のサーバがネットワークで接続する場合のブロック図である。

【図３】図２におけるデータベースまたはサーバ情報管理テーブルに記録されるクライアント認証テーブルの例を示す説明図である。

【図４】図２におけるデータベースまたはサーバ情報管理テーブルに記録されるマシンＩＤ管理テーブルの例を示す説明図である。

【図５】本実施の形態の基本処理シーケンスを示す説明図である。

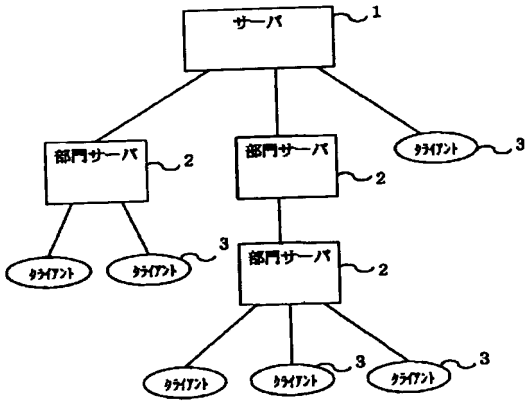
【図６】本実施の形態のマシンＩＤのバックアップ／回復処理のシーケンスを示す説明図である。

【図７】本実施の形態のマシンＩＤの削除処理のシーケンスを示す説明図である。

【符号の説明】

１，１２…サーバ、２…部門サーバ、３，２１…クライアント、１１…ネットワーク、１３…クライアント認証処理部、１４…マシンＩＤ制御部、１５…プログラム・データ送信処理部、１６…データベース、１７…サーバ情報管理テーブル、１８…管理テーブルアクセス部、１９，２８…操作端末、２２…クライアント認証要求部、２３…マシンＩＤ削除要求部、２４…クライアント情報管理テーブル、２５…バックアップ取得部／回復部、２６…プログラム・データ受信処理部、２７…外部装置。

【図１】



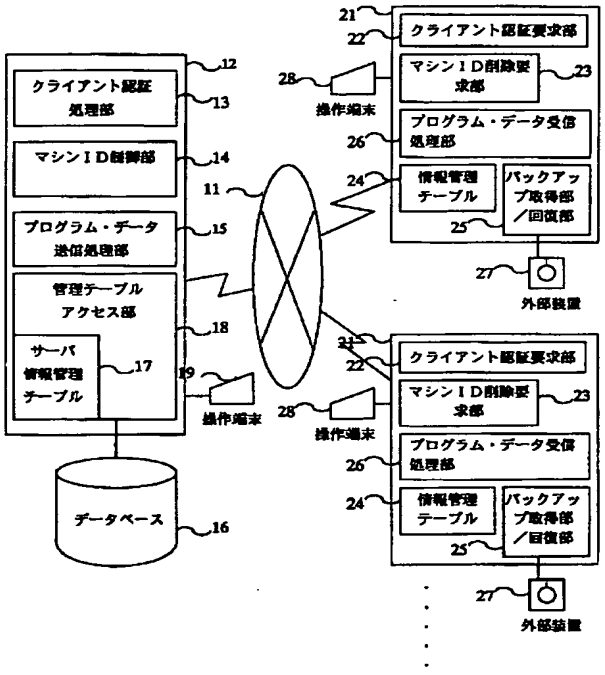
【図３】

クライアント認証テーブル

#	ユーザID	パスワード	実行許可業務
1	U0001	abcd	配布、DBアクセス
2	U0002	xxxx	配布
3	U0003	xyz	DBアクセス
4	U0004	なし	配布、DBアクセス
5	・	・	・
6	・	・	・

31　32　33

【図２】

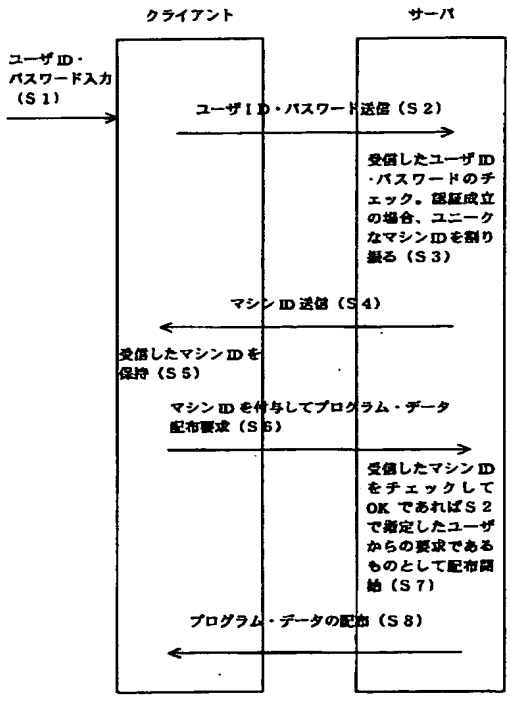


【図４】

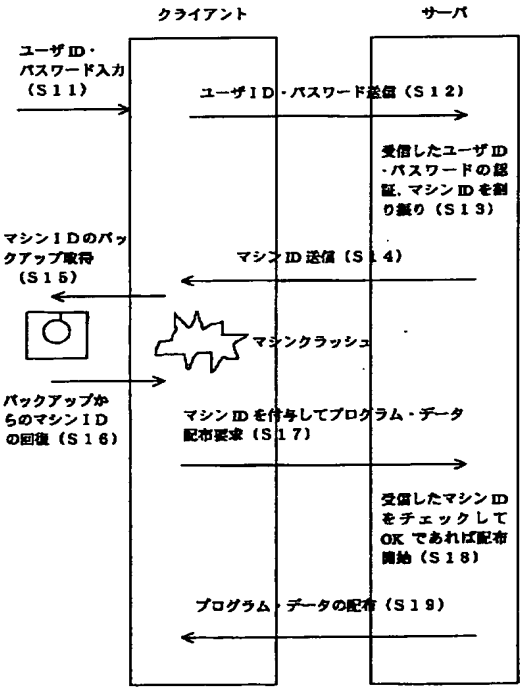
マシンＩＤ管理テーブル

#	マシンＩＤ	ユーザＩＤ	パスワード
1	M0001	U0001	abcd
2	M0002	U0001	abcd
3	M0003	U0003	xyz
4	M0004	U0004	なし
5	・	・	・
6	・	・	・

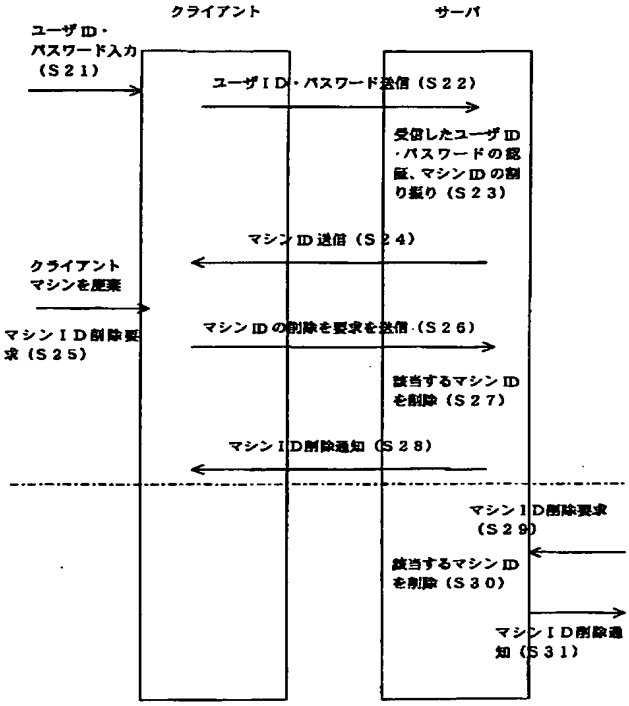
【図５】



【図６】



【図７】


クライアント
サーバ
ユーザID・パスワード入力（Ｓ２１）
ユーザＩＤ・パスワード送信（Ｓ２２）
受信したユーザID・パスワードの認証、マシンIDの割り振り（Ｓ２３）
マシンID送信（Ｓ２４）
クライアントマシンを起案
マシンＩＤ削除要求（Ｓ２５）
マシンIDの削除を要求を送信（Ｓ２６）
該当するマシンIDを削除（Ｓ２７）
マシンＩＤ削除通知（Ｓ２８）
マシンＩＤ削除要求（Ｓ２９）
該当するマシンIDを削除（Ｓ３０）
マシンＩＤ削除通知（Ｓ３１）

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the authentication approach in the system to which the computer which attests, and the computer by which plurality is attested were connected in the network. In the user ID inputted in said computer attested, the step which transmits a password to said computer to attest, and said computer to attest The step which attests that said user ID which received, and a password are the things of a valid user, and when it is attested with a valid user After transmitting the step which transmits the machine ID which is the identifier which specifies said computer attested, and said machine ID to said computer attested from said computer to attest The authentication approach by the machine ID characterized by having the step which attests said computer attested by transmitting said machine ID to the computer which performs said authentication from said computer attested.
[Claim 2] The user ID into which the computer which attests, and the computer by which plurality is attested are the authentication approaches in the system connected in the network, and were inputted in said computer attested, and the step which transmits a bond to said computer to attest, The step which attests the user of said user ID with the received bond in said computer to attest, and when it is attested with a valid user After transmitting the step which transmits the machine ID which is the identifier which specifies said computer attested, and said machine ID to said computer attested from said computer to attest The authentication approach by the machine ID characterized by having the step which attests said computer attested by transmitting said machine ID to the computer which performs said authentication from said computer attested.
[Claim 3] Said computer which received said machine ID from said computer attested in claim 1 or claim 2 and to attest is the authentication approach by the machine ID which recognizes the authentication demand former user when assigning the machine ID concerned, and is characterized by confirming whether the demanded business is the execute permission business of the user concerned while attesting said machine ID.
[Claim 4] The authentication approach by the machine ID characterized by having the step which acquires backup of said machine ID, and the step which recovers Machine ID from this backup in claim 1 or claim 2.
[Claim 5] The authentication approach by the machine ID characterized by having the step which deletes said machine ID registered into said computer to attest in claim 1 or claim 2 by actuation from said computer side to attest or said computer side attested.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention is the environment where access the machine of the side which performs authentication from the near machine by which the plurality distributed on the network is attested, and business is performed, and relates to the authentication approach attested by the meaning machine ID (identifier) assigned per machine of the side attested.
[0002]
[Description of the Prior Art] When performing business in this environment with the spread of the Internet / intranet environments in recent years, about a program, distribution of data, etc., the gestalt to which a client user or a client system distributes the inquiry response mold with which a server side answers to the inquiry by publishing an inquiry actively to a server side has been increasing from the gestalt conventionally distributed from the server side in broadcasting to two or more client sides.
[0003] With such a gestalt, in case a client (side attested) performs a distribution request to a server (side to attest) through a network, it has the need (client authentication is received) of proving its own justification. About the authentication approach of the client in a network, for example like the "security method" of JP,2-16669,A, the user ID and the password which the user of a client side entered are transmitted to a server side, it is checking the contents by the server side, and there is a method of proving the justification of a client. It has this machine authentication and program to the machine concerned and distribution of data are realized. Moreover, like the "user authentication method" of JP,5-35678,A, in order to raise the confidentiality of a password, there is a method whose log in is enabled without pouring a password on a network. [0004]
[Problem(s) to be Solved by the Invention] Thus, since it is necessary to receive distribution authentication to a server side each time when performing an activation demand of business, for example, the distribution request of a program or data, from a client to a server side in the Internet / intranet environment, the user of a client side surely needs to log in by the user ID (or user ID and a password) registered into the database by the side of a server for every time of a distribution request. In order for circuit traffic to distribute at little Nighttime to distribute to a client at this time, for example, a mass program, an operator logs in and does a distribution request in the dead of night, or the client machine is changed into the log in condition (authentication is finished) with the user ID and the password attested between midnight, and it is necessary to perform a distribution request to a server from a client automatically to the timing of arbitration. However, as for the former, the latter has a security top problem on employment.
[0005] Moreover, in the case of a program or data distribution, the function which attests not a user (man) but the computer itself which logs in to the computer which there are needs to make it the form distributed to the computer instead of a user (man) of a client (the user who can log in to that computer owns jointly, and use/reference is possible for him), and is attested at this time by the server side is required. However, the authentication approach of the client machine itself is not described by the two above-mentioned approaches.
[0006] In the environment where client authentications [purpose / of this invention], such as the Internet/intranet, are indispensable An operator logs in in the dead of night. Require activation of business of a server or Without using an approach with the problem on employment of changing the

client machine into the log in condition with the user ID and the password attested between midnight, and requiring activation of business to the timing of arbitration, or security It is in offering the authentication approach that make unnecessary log in actuation with the user ID and the password for every operating activation demand, and distribution to the uninhabited terminal at night which needs authentication also enables operating employment of operator loess.
[0007] Other purposes of this invention are to offer the authentication approach which can attest not the user (man) of a client but the calculating machine of a client itself by the server side.
[0008]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, invention concerning claim 1 It is the authentication approach in the system to which the computer which attests, and the computer by which plurality is attested were connected in the network. In the user ID inputted in said computer attested, the step which transmits a password to said computer to attest, and said computer to attest The step which attests that said user ID which received, and a password are the things of a valid user, and when it is attested with a valid user After transmitting the step which transmits the machine ID which is the identifier which specifies said computer attested, and said machine ID to said computer attested from said computer to attest It is characterized by having the step which attests said computer attested by transmitting said machine ID to the computer which performs said authentication from said computer attested.
[0009] Invention concerning claim 2 is the authentication approach in the system to which the computer which attests, and the computer by which plurality is attested were connected in the network. In the user ID inputted in said computer attested, the step which transmits a bond to said computer to attest, and said computer to attest The step which attests the user of said user ID with the received bond, and when it is attested with a valid user After transmitting the step which transmits the machine ID which is the identifier which specifies said computer attested, and said machine ID to said computer attested from said computer to attest It is characterized by having the step which attests said computer attested by transmitting said machine ID to the computer which performs said authentication from said computer attested.
[0010] Said computer by which invention concerning claim 3 received said machine ID from said computer attested in claim 1 or claim 2 and to attest is characterized by recognizing the authentication demand former user when assigning the machine ID concerned, and confirming whether the demanded business is the execute permission business of the user concerned while it attests said machine ID.
[0011] Invention concerning claim 4 is characterized by having the step which acquires backup of said machine ID, and the step which recovers Machine ID from this backup in claim 1 or claim 2.
[0012] Invention concerning claim 5 is characterized by having the step which deletes said machine ID registered into said computer to attest by actuation from said computer side to attest or said computer side attested in claim 1 or claim 2.
[0013]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained, referring to a drawing.
[0014] Drawing 1 is the client / server structure-of-a-system Fig. for applying the authentication approach by the machine ID concerning this invention. In drawing 1 , 1 is located in the high order of each section server or a client, and is a subordinate's section server and a server which performs authentication of a client. The section server which 2 receives authentication in the server of a high order, and performs authentication of a subordinate's section server or a client, and 3 are clients which receive authentication in the server and section server of a high order. This invention can be applied when it is versatility to be attested when a client 3 receives authentication in the server 1 of the high order, a client 3 receives authentication in the section server 2 of the high order and the section server 2 receives authentication in the server 1 of the high order, and when the section server 2 receives authentication in the section server 2 of the high order. What is necessary is just to apply other configurations and procedure with the same said of a case henceforth [drawing 2], below, although the case where a client receives authentication in the server of a high order is explained to an example.
[0015] Drawing 2 is drawing showing the example of a configuration in case one set or two or more

sets of the clients 21 which perform the distribution request of a program or data, and the server 12 that attests this client in advance of distribution at the time of the distribution-request reception from this client are connected through the network 11 as a gestalt of 1 operation of this invention.

[0016] In drawing 2 , the network which 11 connects physically and logically between the server mentioned later or a client, and serves as a medium of various program data distributions, and 12 are servers which perform authentication processing of a client, program to a client, and transmitting processing of data. When the user ID and the password sent from the client are attested, the client authentication processing section which attests the user ID and the password with which 13 has been sent from the client, and Machine ID, and 14 The machine ID control section which assigns Machine ID, the program data transmitting processing section to which 15 transmits a program and data according to the distribution request from a client, The database with which 16 stores the information on client authentication or program data distribution as an external device, The server information management table which stores the information in which a database 16 stores 17 on the primary storage and memory of a server, The managed table access section which performs access to the server information management table 17 stored on the primary storage and memory in the database 16 whose 18 is an external device, or a server, 19 is an operating station for a server manager etc. to update and refer to information, such as a client authentication table and a machine ID managed table.

[0017] Moreover, 21 is a client which performs the own authentication demand of a client and the distribution request of program data to a server 12. 22 is the client authentication demand section which requires authentication of a server by the user ID and the password entered by the client user, and the machine ID assigned by the server 12 after authentication. The machine ID deletion demand section which requires deletion of the machine ID by which 23 was once assigned from the server 12 of a server side, the information (user ID and a password --) concerning [24] a client user and a client machine Back up the client information management table which manages Machine ID, and the machine ID by which 25 was assigned from the server 12 to the external devices 27, such as FD (floppy disk), or The backup acquisition section / recovery section which recovers Machine ID from backup of an external device 27 on the contrary, The program data reception section which carries out reception of what 26 required a program and distribution of data from the server 12, and has actually been distributed from the server 12, The external device in which 27 stores backup of Machine ID, and 28 are the operating stations for directing activation of the backup to the external device 27 of the machine ID by which the client user was assigned from the server 12, recovery from an external device 27, deletion of Machine ID, etc.

[0018] Drawing 3 is the example of the client authentication table for attesting the user ID and the password sent from the client 21 in the authentication approach by the machine ID concerning this invention applied to the configuration of drawing 2 . A client authentication table includes the operating list (33) which permits authorized user ID (31), a password (32), and activation for authentication. A client authentication table is a table which it is held at the database 16 of drawing 2 R> 2, it is loaded on main memory as one of the server information management tables 17, and is accessed.

[0019] Drawing 4 is the example of the machine ID managed table for attesting the machine ID sent from the client in the authentication approach by the machine ID concerning this invention applied to the configuration of drawing 2 . A machine ID managed table contains the requiring agency user ID (42) when assigning the machine ID (41) assigned to each client machine and Machine ID, and a password (43). A machine ID managed table is a table which it is held at the database 16 of drawing 2 , it is loaded on main memory as one of the server information management tables 17, and is accessed.

[0020] Drawing 5 shows the procedure for receiving authentication from a server 12 by the authentication approach by the machine ID which requires for this invention the client 21 connected through the network 11 like drawing 2 , and receiving distribution of the program data to demand. As shown in this drawing, a client user or the setup manager of a client machine enters user ID and a password in a client 21 first (S1). A client 21 enciphers the entered user ID and the password at the time of the 1st distribution request, and transmits to a server 12 (S2). In the 1st time, it is a time of receiving a program and distribution of data at the beginning of No. 1, and setting them up in a

client. That is, when setting up a program and data first, it attests with user ID and a password, and it attests with mentioning later after it by Machine ID. In addition, an original data scramble method is sufficient as the method of encryption also in the method of international standards.

[0021] The server 12 which received user ID and a password confirms whether its user ID and password are registered into the client authentication table in a database 16 or the server information management table 17 on an internal memory (drawing 3) after the decryption, and "distribution" is included in execute permission business (S3). When its user ID and password have obtained distribution authorization in accordance with the registered thing as a result of the check, it attests that it is a just client, the unique machine ID is assigned, and the machine ID, and the user ID and the password which were attested are registered into the machine ID managed table in a database 16 or the server information management table 17 on an internal memory (drawing 4) (S3). In this case, even if it already assigns Machine ID with the received user ID and the password and is ending, the meaning machine ID can newly be assigned. In addition, an original data scramble method is sufficient as the method of encryption also in the method of international standards.

[0022] Next, a server 12 enciphers the assigned machine ID and transmits to a client 21 (S4). In addition, when not in agreement with what has registered user ID and password, it notifies to a client 21 that authentication went wrong.

[0023] The client 21 which client authentication was successful and received the unique machine ID holds the contents in the client information management table 24 after a decryption (S5).

[0024] Then, to a server 12, a client 21 gives Machine ID and transmits the distribution request of a program or data (S6). In addition, what is necessary is to give Machine ID and just to transmit a distribution request, when requiring a program and distribution of data of a server from the client concerned after Machine ID is assigned. For example, what is necessary is just to construct the schedule of taking out automatically the machine ID currently held in the client information management table 24, giving the machine ID, and transmitting a distribution request to distribute automatically in program, when there is little traffic, such as midnight. It can perform giving Machine ID and performing a distribution request automatically in the condition of not logging in, for example.

[0025] As for the server 12 which received the distribution request to which Machine ID was given, the machine ID confirms whether register with the machine ID managed table in a database 16 or the server information management table 17 on an internal memory (drawing 4) (S7). When in agreement with a thing with the registered machine ID as a result of a check, it attests that it is a just client (S7). At this time, it asks for the user ID of the demand origin corresponding to the machine ID concerned with reference to a machine ID managed table (drawing 4), the execute permission business permitted to the user of that user ID from the client authentication table (drawing 3) is searched for, and it confirms whether to be what the business demanded from the client is permitted. If a program and distribution of data are permitted, they will distribute a program and data with a demand to the client 21 concerned the demanded business and here (S8).

[0026] Drawing 6 shows the procedure at the time of recovery from acquisition and backup of backup of the machine ID received after the client 21 connected through the network 11 like drawing 2 received authentication from a server 12 by the authentication approach by the machine ID concerning this invention. Since the procedure of S11-S14 is the same as S1 of drawing 5 - S4 as shown in this drawing, explanation is omitted.

[0027] The client 21 which client authentication was successful and received the unique machine ID backs up the contents to external devices, such as FD, after a decryption (S15). FD which backed up Machine ID is kept by the client user concerned.

[0028] When the assigned machines ID, such as crash of a client machine, were destroyed, or when changing the machine which a client user uses, the machine [finishing / server authentication] ID is recovered from external devices, such as FD which backed up Machine ID, (S16). Then, when transmitting a distribution request to a server 12, the recovered machine ID is given and a distribution request is transmitted (S17). Processing of S17-S19 is the same as S6-S8 of drawing 5 .

[0029] Drawing 7 shows the procedure of deleting Machine ID from on the procedure of requiring deletion of Machine ID of a server 12 from a client 21, and a server 12, by abandonment of a client machine etc., after the client 21 connected through the network 11 like drawing 2 receives

authentication from a server 12 by the authentication approach by the machine ID concerning this invention. Since the procedure of S21-S24 is the same as S1 of drawing 5 - S4 as shown in this drawing, explanation is omitted.

[0030] Client authentication is successful, and in the client 21 which received the unique machine ID, when need, such as abandonment of the client machine concerned, arises after that, a client user or the setup manager of a client machine demands deletion of the machine ID assigned to self from the operating station of a server side (S25). In response to the directions, a client 21 transmits the deletion demand of Machine ID to a server 12 side (S26).

[0031] The server 12 which received the deletion demand of Machine ID deletes the machine ID which the machine ID confirms whether register with the machine ID managed table in a database 16 or the server information management table 17 on an internal memory (drawing 4), and corresponds if registered (S27). The server 12 which deleted Machine ID notifies deletion of Machine ID to a client 21 side (S28).

[0032] On the other hand, when the deletion demand of Machine ID cannot be performed from the client machine side concerned in crash of a client machine etc., the system administrator by the side of a server demands deletion of the machine ID concerned from the operating station of a server 12 directly (S29). The server 12 which received the deletion demand of Machine ID deletes the machine ID which the machine ID by which the deletion demand was carried out confirms whether register with the machine ID managed table in a database 16 or the server information management table 17 on an internal memory (drawing 4), and corresponds if it exists (S30). The server 12 which deleted Machine ID notifies deletion of Machine ID on the operating station of the system administrator by the side of a server (S31).

[0033] Since according to the gestalt of the above-mentioned implementation a requiring agency user when the server which received Machine ID assigns the machine ID concerned is recognized and the demanded business is confirming whether to be the business permitted to the user, a server can perform business as what is the operating activation demand from the user concerned.

[0034] Furthermore, also when the client which had Machine ID assigned from the computer attested once crashes, re-acquisition of the machine ID by the user ID and password, or bond from a client can be made unnecessary by recovering Machine ID from the backup beforehand acquired to external devices, such as FD.

[0035] Moreover, when the client which had Machine ID once assigned from a server is crashed or discarded, deletion of Machine ID can be performed by actuation from a server side or a client side so that the machine ID which became unnecessary at the server side may not be made to remain.

[0036] In addition, although the gestalt of the above-mentioned implementation explained the example which performs the first authentication with user ID and a password, in addition to it instead of authentication with user ID and a password, the authentication approach by the bond may be used. A bond is data (data made into the form which cannot be forged by the so-called digital signature) which enciphered the public key of the owner of the bond with some information, such as user ID, using the private key of a certificate authority, for example. With the certificate (public key) of a certificate authority, the others are checking the digital signature of this bond, and can check the justification of the bond.

[0037]

[Effect of the Invention] Since he is trying for 2nd henceforth to receive the authentication over an activation demand of business using the machine ID assigned at the time of first-time authentication, according to this invention, the client machine which received authentication in the first-time demand to a server with user ID and a password in the authentication approach for the operating activation demand to the server machine from the client machine currently distributed through a network can make unnecessary the log in actuation with the user ID and the password for every operating activation demand. Therefore, distribution to the uninhabited terminal of Nighttime which needs authentication also enables operating employment of operator loess, without using an approach with the problem on employment that log in in the dead of night, and require activation of business of a server, or the operator changes the client machine into the log in condition with the user ID and the password attested between midnight, and demands activation of business to the timing of arbitration, or security. Moreover, not the user (man) of a client but the calculating

machine of a client itself can be attested by the server side.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] They are the client / server structure-of-a-system Fig. for performing authentication by the machine ID of this invention.
[Drawing 2] It is a block diagram in case one set of a server connects with one set of a client as a gestalt of operation of this invention in a network.
[Drawing 3] It is the explanatory view showing the example of the client authentication table recorded on the database or server information management table in drawing 2 .
[Drawing 4] It is the explanatory view showing the example of the machine ID managed table recorded on the database or server information management table in drawing 2 .
[Drawing 5] It is the explanatory view showing the primitive operation sequence of the gestalt of this operation.
[Drawing 6] It is the explanatory view showing the sequence of backup/recovery of the machine ID of the gestalt of this operation.
[Drawing 7] It is the explanatory view showing the sequence of the deletion of the machine ID of the gestalt of this operation.
[Description of Notations]
1 12 [-- Network,] -- A server, 2 -- 3 A section server, 21 -- A client, 11 13 -- The client authentication processing section, 14 -- A machine ID control section, 15 -- Program data transmitting processing section, 16 -- A database, 17 -- A server information management table, 18 -- Managed table access section, 19 28 [-- A client information management table, 25 / -- The backup acquisition section / recovery section, 26 / -- The program data reception section, 27 / -- External device.] -- An operating station, 22 -- The client authentication demand section, 23 -- The machine ID deletion demand section, 24

[Translation done.]